採用融合存取的整合存取無線LAN控制器訪客錨點組態範例

目錄

簡介

本檔案介紹如何在新的行動化部署設定中設定無線使用者端訪客錨點的5508/5760系列無線LAN控制器(WLC)和Catalyst 3850系列交換器，其中5508系列WLC作為行動錨點，Catalyst 3850系列交換器作為使用者端的行動化外部控制器。此外，Catalyst 3850系列交換器擔任行動代理，以連線至用作行動控制器的5760系列WLC，Catalyst 3850系列交換器會從其中取得存取點(AP)授權。

必要條件

需求

思科建議您在嘗試此設定之前瞭解以下主題：

- 採用融合接入5760和3650系列WLC和Catalyst 3850系列交換機的思科IOS® GUI或CLI
- 5508系列WLC的GUI和CLI訪問
- 服務組識別碼(SSID)配置
- Web驗證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5760版本3.3.3（下一代配線間[NGWC]）
- Catalyst 3850系列交換器
- Cisco 5508系列WLC版本7.6.120
- Cisco 3602系列輕量AP
- Cisco Catalyst 3560 系列交換器

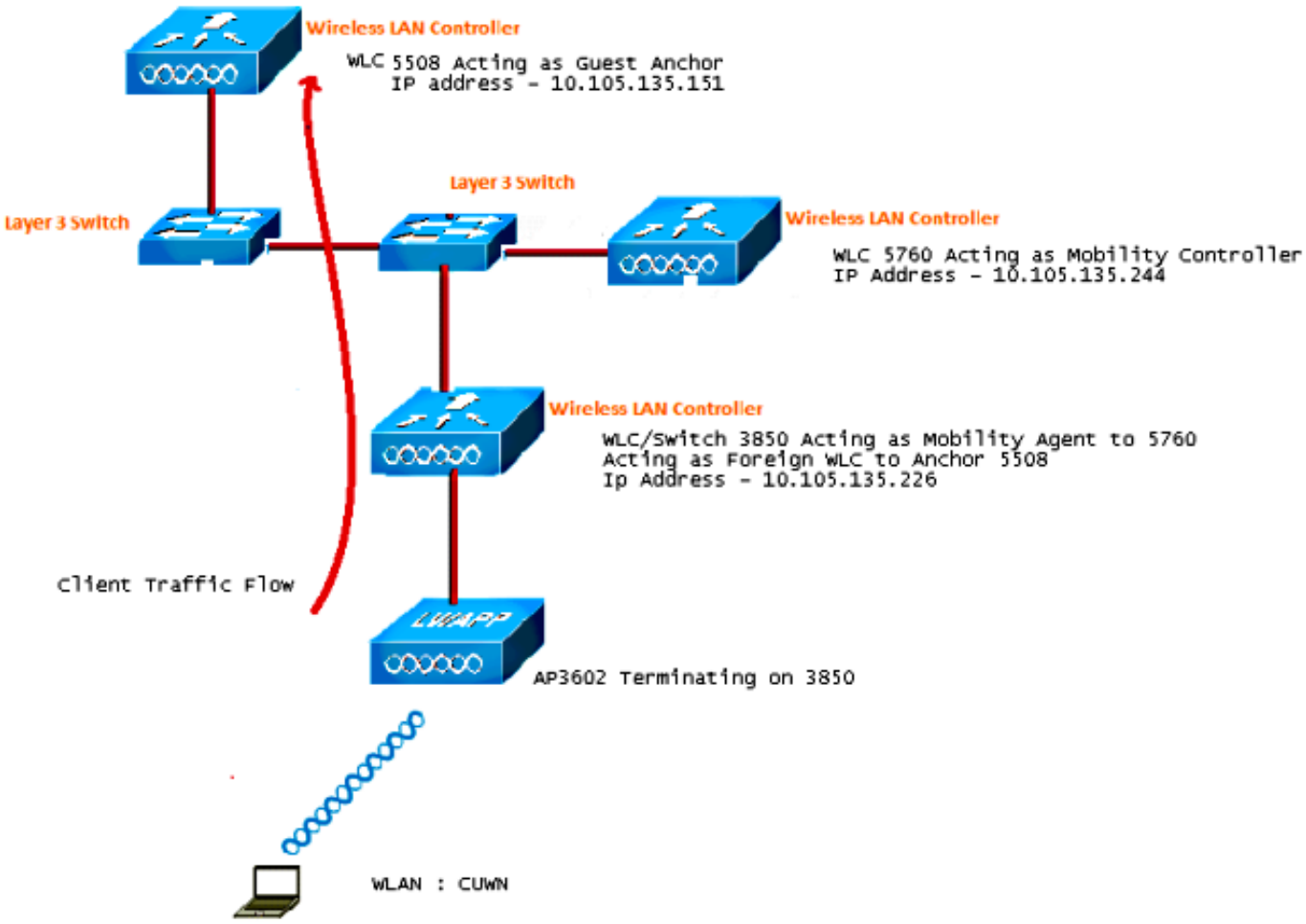
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

註：使用命令查詢工具(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

5508系列WLC擔任錨點控制器，Catalyst 3850系列交換器擔任外部控制器和行動代理（從行動控制器5760取得授權）。



註：在網路圖中，5508系列WLC用作錨點控制器，5760系列WLC用作移動控制器，Catalyst 3850系列交換機用作移動代理和外部WLC。在任何時間點，Catalyst 3850系列交換器的錨點控制器是5760系列WLC或5508系列WLC。兩者不能同時是錨點，因為雙錨點不起作用。

組態

該配置包括三個部分：

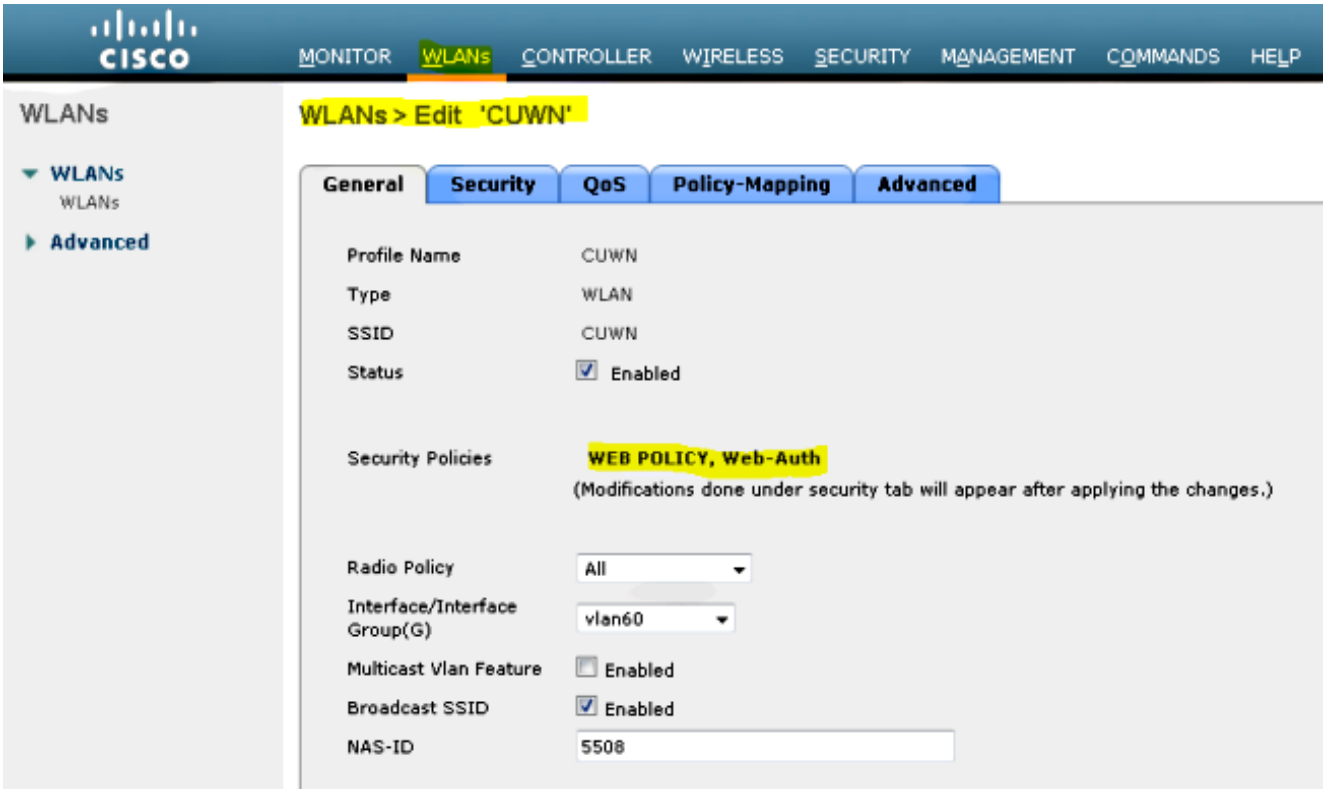
[第1部分 — 5508錨點WLC上的配置]

[第2部分 — 5508/5760系列WLC和Catalyst 3850系列交換機之間的融合接入移動配置]

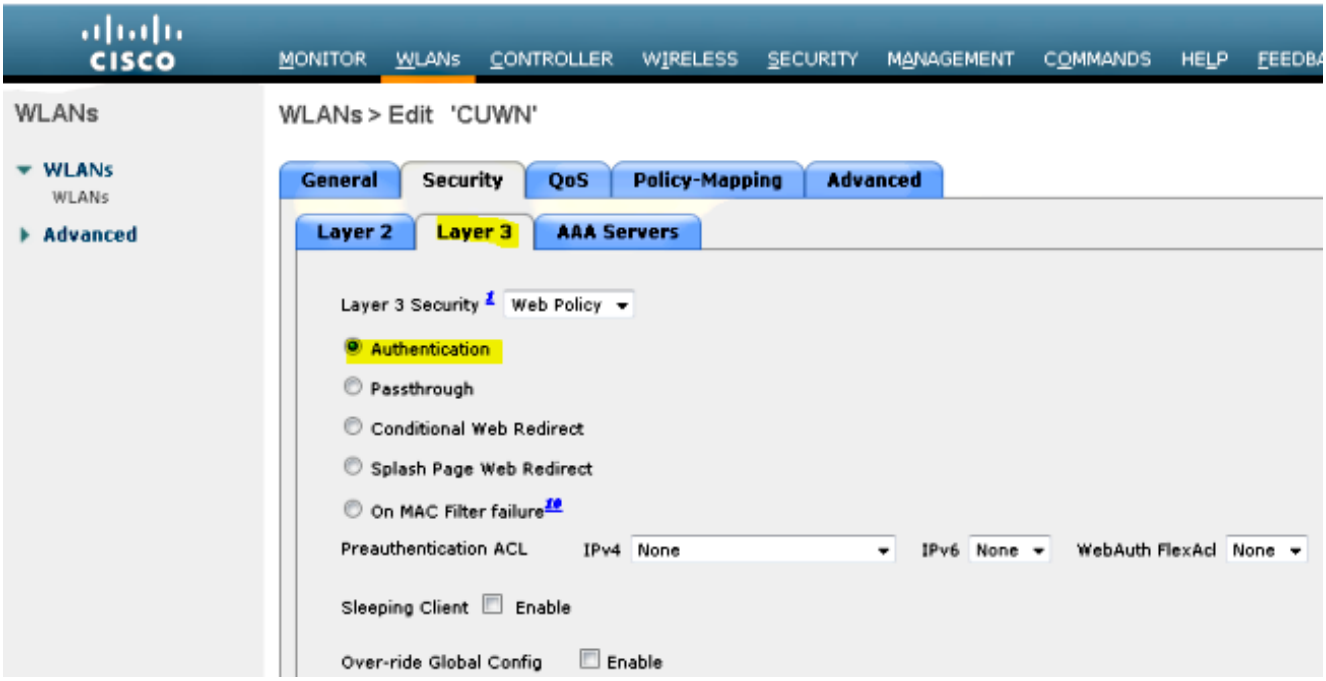
[第3部分 — 外部Catalyst 3850系列交換機的配置]

第1部分 — 5508錨點WLC上的配置

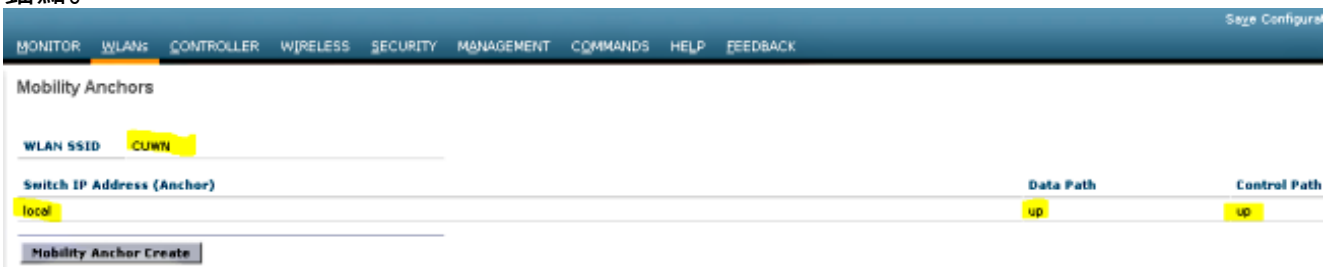
1. 在5508系列WLC上，將滑鼠懸停在**WLAN > New**上以建立新的無線LAN(WLAN)。



2. 將滑鼠懸停在**WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication**上，以配置第3層安全性。



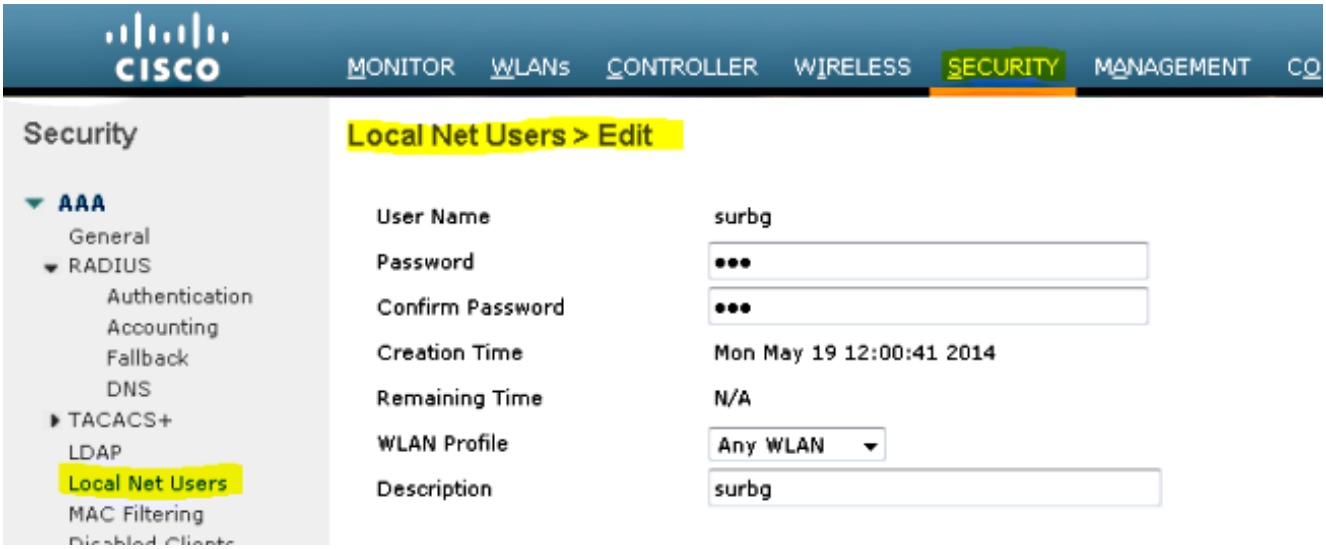
3. 在WLAN Mobility Anchor configuration視窗下將錨點位址**local**，以便將5508系列WLC新增為錨點。



4. 將滑鼠懸停在**Security > Webauth > Webauth page**上，以配置用於客戶端身份驗證的Webauth頁面。

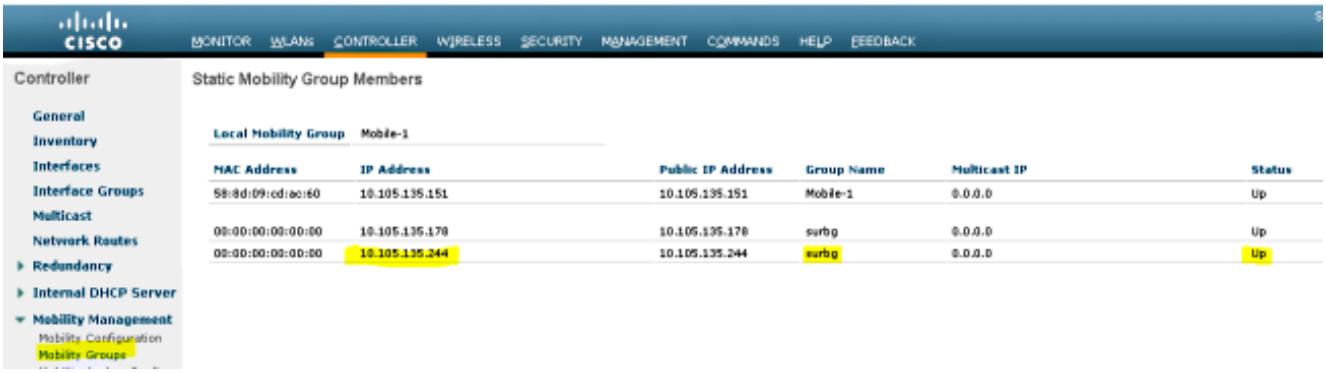
   在此範例中，選擇WLC內部Webauth頁面：

5. 建立本地網路使用者。此使用者名稱/密碼對是在Webauth頁面上出現提示時由使用者使用。

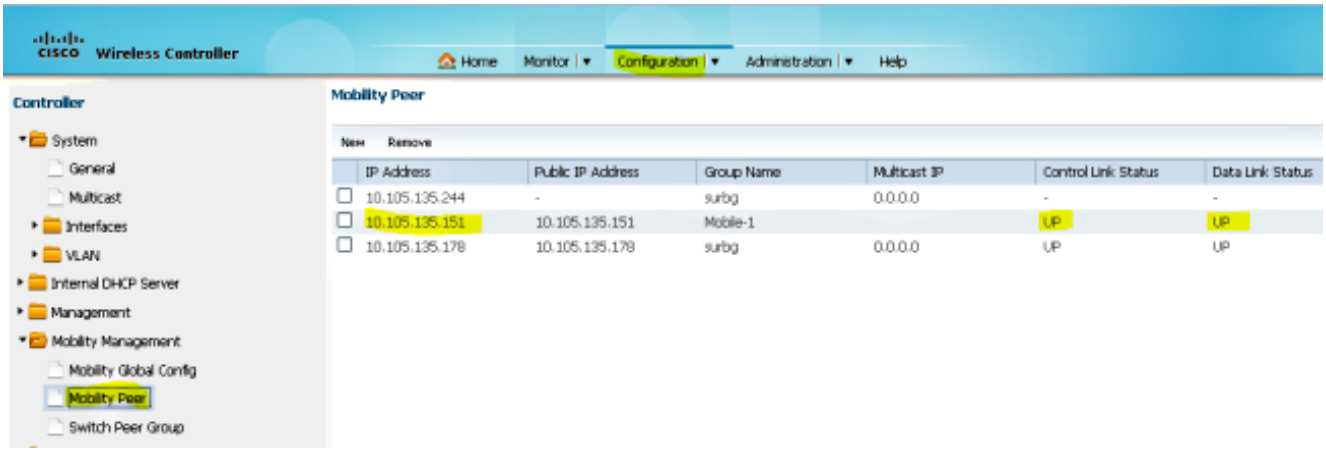


第2部分 — 5508/5760系列WLC和Catalyst 3850系列交換機之間的融合接入移動配置

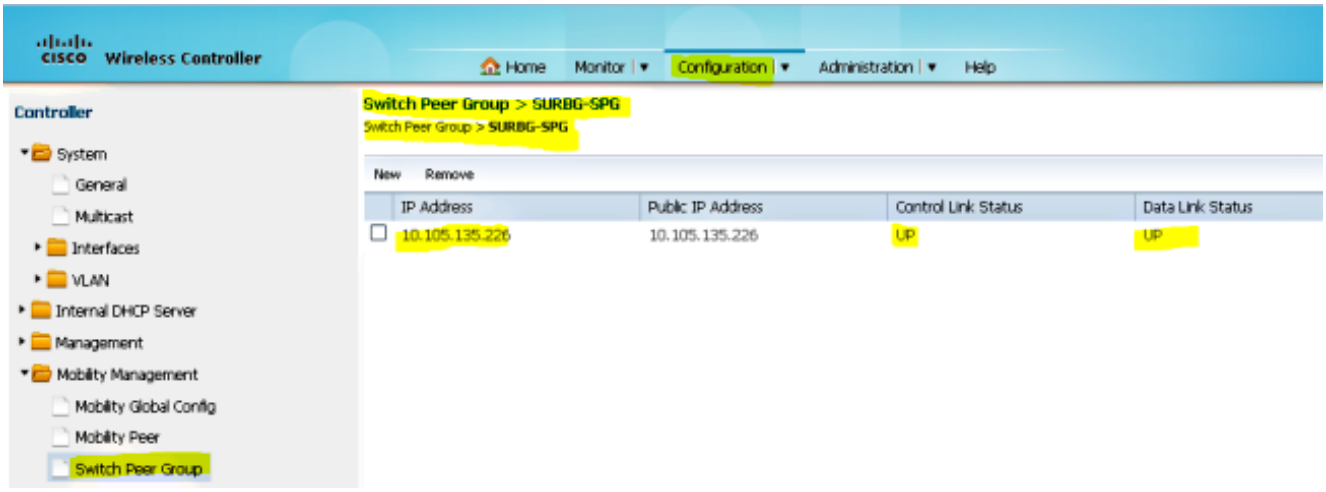
1. 在5508系列WLC上，將5760系列WLC新增為行動對等點。



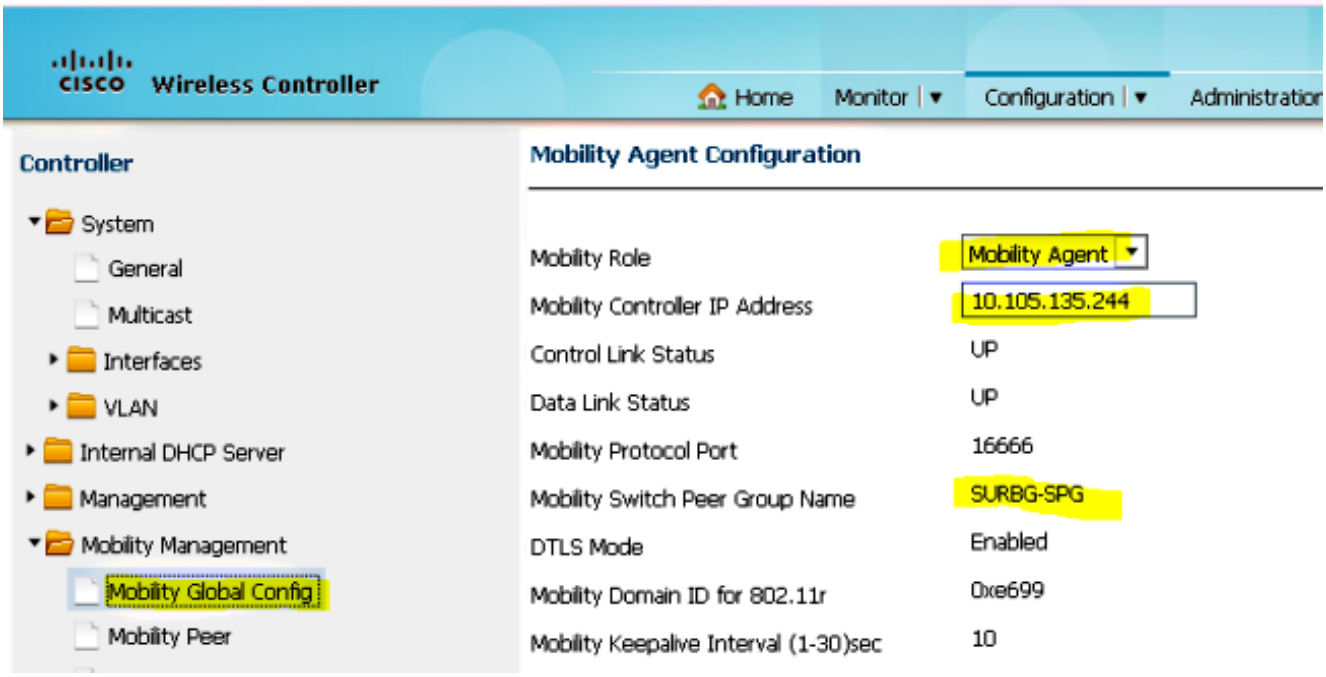
2. 在5760系列WLC上，作為行動控制器，將5508系列WLC新增為行動對等點。



3. 此步驟非常重要！在Mobility Management下的Switch Peer Group頁籤下，將Catalyst 3850系列交換機作為5760系列WLC上的移動代理新增。



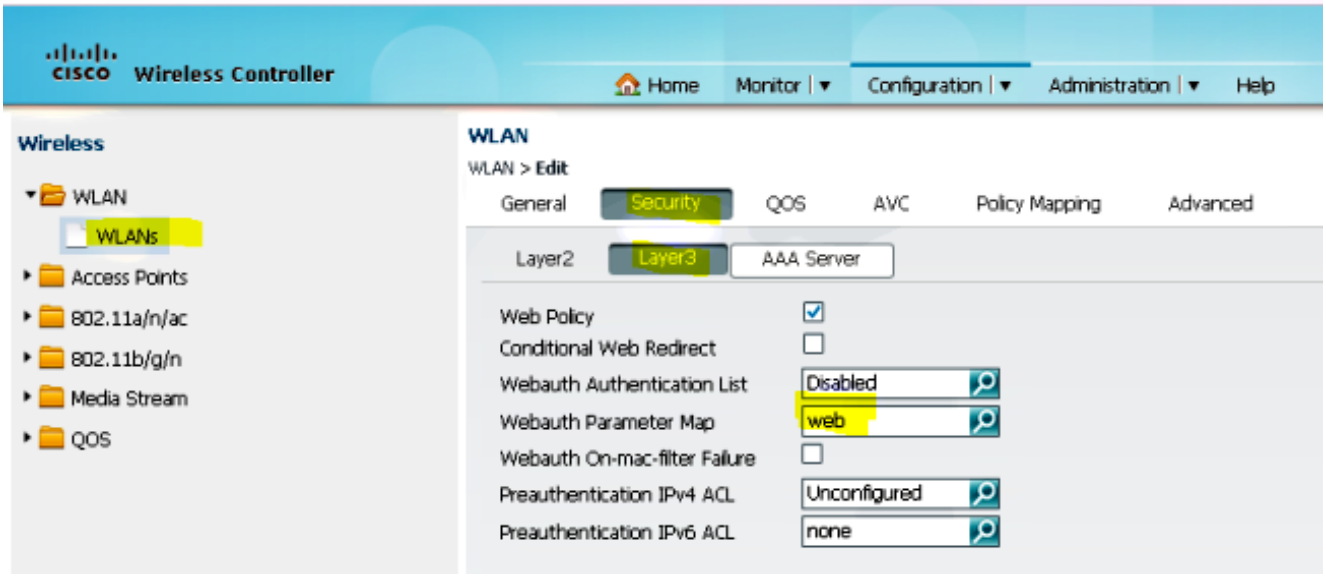
4. 在Catalyst 3850系列交換器上，將5760系列WLC新增為行動控制器。執行此操作後，Catalyst 3850系列交換器會從行動控制器5760取得AP無法授權。



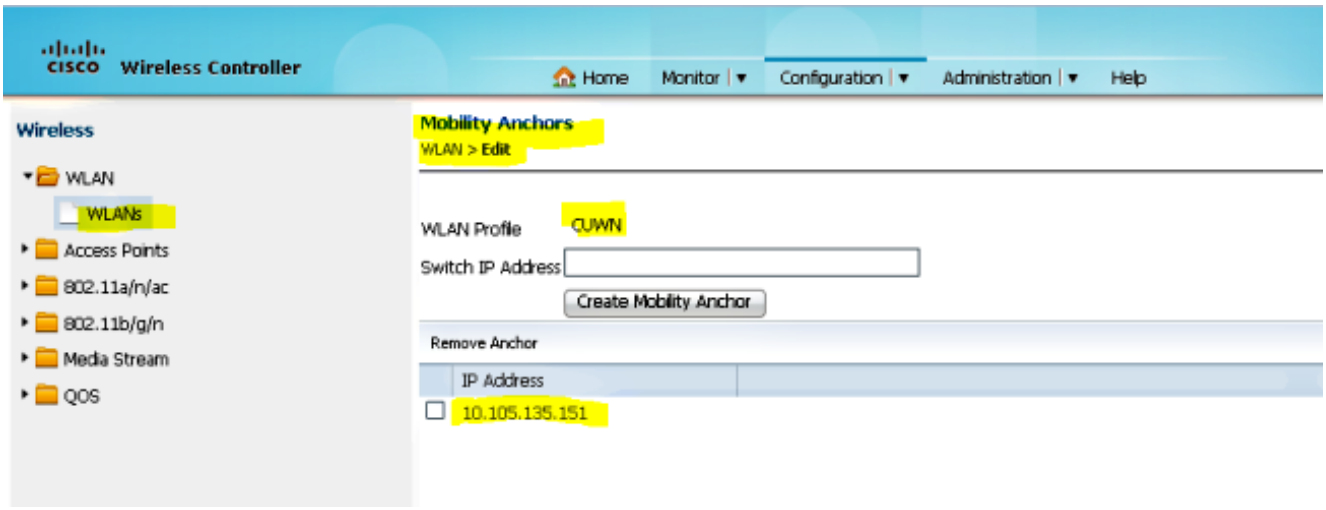
第3部分：外部Catalyst 3850系列交換機的配置

1. 將滑鼠懸停在**GUI > Configuration > Wireless > WLAN > New**上，以便在Catalyst 3850系列交換機上配置準確的SSID/WLAN。

2. 將滑鼠懸停在**WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication**上，以配置第3層安全性。



3. 在WLAN行動錨點設定下將5508系列WLC IP位址新增為錨點

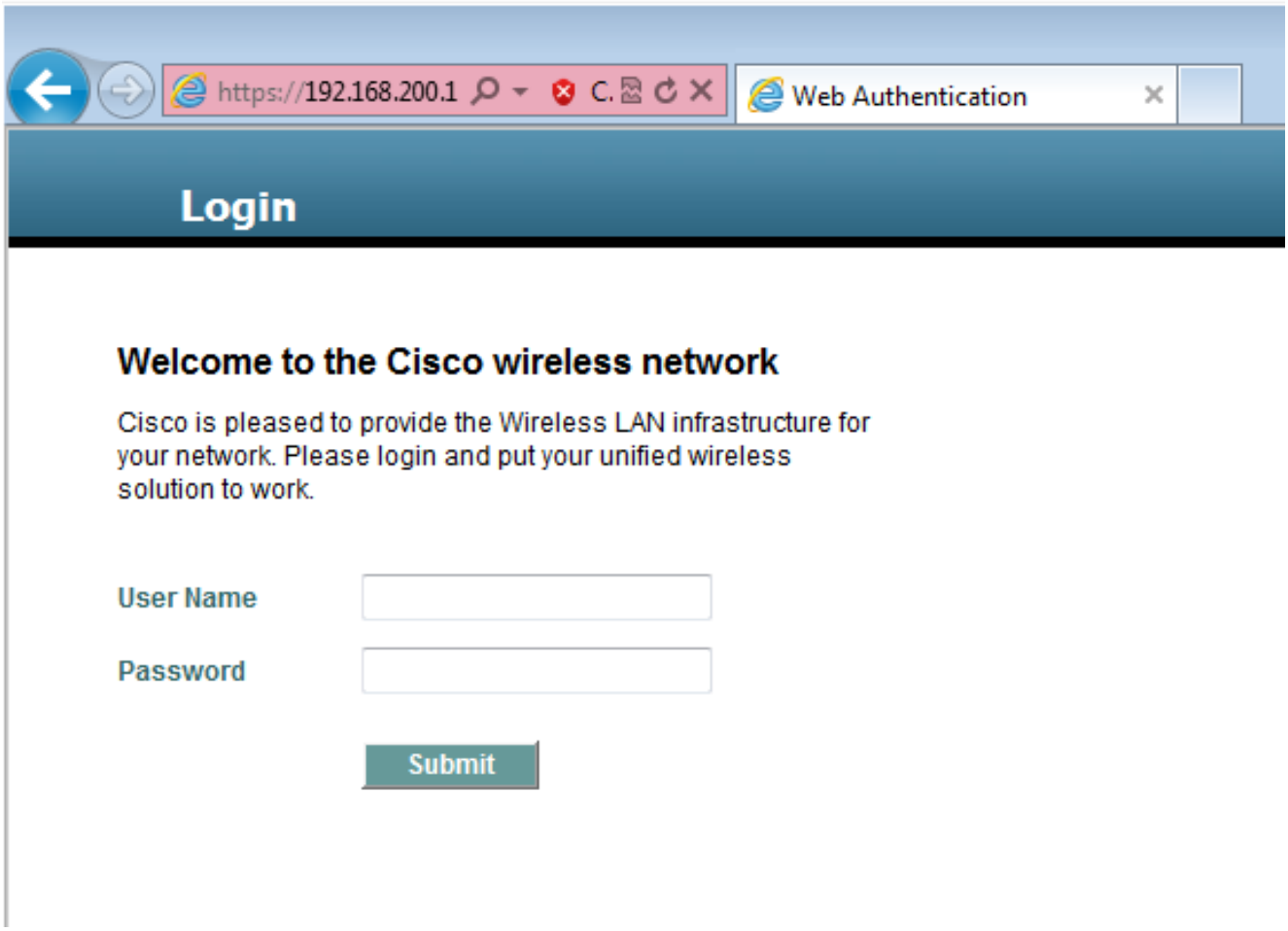


驗證

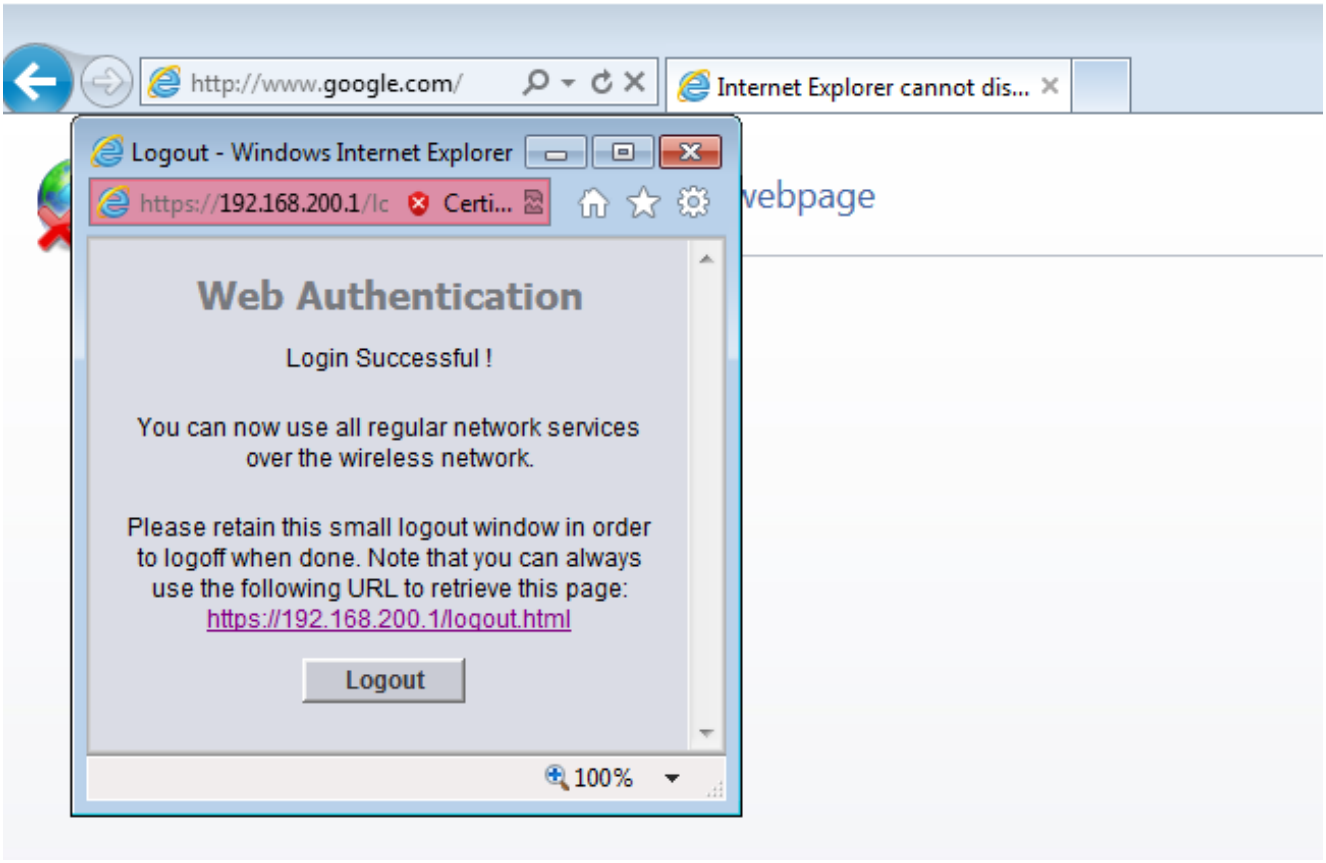
使用本節內容，確認您的組態是否正常運作。

將使用者端連線到WLAN思科整合無線網路(CUWN)。工作流程如下：

1. 客戶端收到IP地址。
2. 客戶端開啟瀏覽器並訪問任何網站。
3. 使用者端傳送的第一個TCP封包會被WLC劫持，WLC會攔截並傳送Webauth頁面。
4. 如果DNS設定正確，使用者端會取得Webauth頁面。
5. 使用者端必須提供使用者名稱/密碼才能進行驗證。
6. 成功驗證後，使用者端將被重新導向到原始存取頁面。



7. 使用者端提供正確憑證後，使用者端會傳遞驗證。



疑難排解

若要對組態進行疑難排解，請在5508系列WLC上（充當訪客錨點）輸入以下偵錯：

```
Debug Client
```

```
Debug web-auth redirect enable mac
```

以下是範例：

```
Debug Client 00:17:7C:2F:B6:9A
Debug web-auth redirect enable mac 00:17:7C:2F:B6:9A

show debug

MAC Addr 1..................................... 00:17:7C:2F:B6:9A

Debug Flags Enabled:
 dhcp packet enabled.
 dot11 mobile enabled.
 dot11 state enabled
 dot1x events enabled.
```

```
 dot1x states enabled.
 FlexConnect ft enabled.
 pem events enabled.
 pem state enabled.
 CCKM client debug enabled.
 webauth redirect enabled.

*mmMaListen: May 19 13:36:34.276: 00:17:7c:2f:b6:9a Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override for default ap group,
marking intgrp NULL
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Applying Interface policy on
Mobile, role Unassociated. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 0

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Re-applying interface policy
for client

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv4
ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2219)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv6
ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2240)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a apfApplyWlanPolicy: Apply WLAN
Policy over PMIPv6 Client Mobility Type
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override from intf group to an
intf for roamed client - removing intf group from mscb


*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 L2AUTHCOMPLETE (4)
Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 acl from
255 to 255

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 Flex acl
from 65535 to 65535

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Stopping deletion of Mobile
Station: (callerId: 53)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Adding
Fast Path rule   type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path
rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local Bridging Vlan = 60,
Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) State
Update from Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor,
client state=APF_MS_STATE_ASSOCIATED
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Change state to DHCP_REQD (7) last state DHCP_REQD (7)

*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 5807, Adding TMP rule
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
```

Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local
Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Sent an XID frame
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Pushing IPv6 Vlan Intf
ID 13: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A ,
Binding to Data Plane. SUCCESS !! dhcpv6bitmap 0
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Calling mmSendIpv6AddrUpdate
for addition of IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , for MAC:
00:17:7C:2F:B6:9A
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a mmSendIpv6AddrUpdate:4800
Assigning an IPv6 Addr fe80:0000:0000:0000:6c1a:b253:d711:0c7f to the client in
Anchor state update the foreign switch 10.105.135.226
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Link Local address fe80::
6c1a:b253:d711:c7f updated to mscb. Not Advancing pem state.Current state: mscb
in apfMsMmInitial mobility state and client state APF_MS_STATE_AS
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of
type 9, dtlFlags 0x4
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Static IP client associated to
interface vlan60 which can support client subnet.
***dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 DHCP_REQD (7)
Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)**

*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
pemAdvanceState2 6717, Adding TMP rule
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Replacing Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Fast Path rule (contd...) 802.1P = 0, **DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13**
***dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)**
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Plumbing web-auth redirect rule
due to user logout
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a apfAssignMscbIpAddr:1148
Assigning an Ip Addr 60.60.60.11 to the client in Anchor state update the foreign
switch 10.105.135.226
*dtlArpTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Assigning Address 60.60.60.11
to mobile
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for

```
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a 60.60.60.11 Added NPU entry
of type 2, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Pushing IPv6:
fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A , Binding to
Data Plane. SUCCESS !!
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Sent an XID frame

(5508-MC) >
(5508-MC) >
(5508-MC) >*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP received
op BOOTREQUEST (1) (len 314,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
           dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
           dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selected relay 1 -
60.60.60.251 (local address 60.60.60.2, gateway 60.60.60.251, VLAN 60, port 1)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
REQUEST (3)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   op: BOOTREQUEST,
htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   xid: 0xad00ada3
(2902502819), secs: 3072, flags: 0
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   chaddr:
00:17:7c:2f:b6:9a
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   ciaddr: 0.0.0.0,
yiaddr: 0.0.0.0
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   siaddr: 0.0.0.0,
giaddr: 60.60.60.2
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   requested ip:
60.60.60.11
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP sending REQUEST to
60.60.60.251 (len 358, port 1, vlan 60)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selecting relay 2 -
control block settings:
           dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
           dhcpGateway: 0.0.0.0, dhcpRelay: 60.60.60.2  VLAN: 60
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selected relay 2 -
NONE (server address 0.0.0.0,local address 0.0.0.0, gateway 60.60.60.251, VLAN 60,
port 1)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP received op BOOTREPLY
(2) (len 308,vlan 60, port 1, encap 0xec00)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP setting server from ACK
(server 60.60.60.251, yiaddr 60.60.60.11)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
ACK (5)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   xid: 0xad00ada3
(2902502819), secs: 0, flags: 0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   chaddr:
00:17:7c:2f:b6:9a
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   ciaddr: 0.0.0.0,
yiaddr: 60.60.60.11
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   siaddr: 0.0.0.0,
giaddr: 0.0.0.0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   server id:
192.168.200.1  rcvd server id: 60.60.60.251
*webauthRedirect: May 19 13:36:47.678: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:47.680: captive-bypass detection disabled, Not
```

checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Preparing redirect URL according to configured Web-Auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Checking custom-web config for WLAN ID:4
***webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- unable to get the hostName for virtual IP, using virtual IP =192.168.200.1**
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Global status is enabled, checking on web-auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type Internal, no further redirection needed. Presenting defualt login page to user
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv= "Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body2 is "></HEAD></HTML>

***webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser host is www.facebook.com**
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser path is /
***webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- added redirect=, URL is now https://192.168.200.1/login.html?**
***webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- str1 is now https://192.168.200.1/login.html?redirect=www.facebook.com/**
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- clen string is Content-Length: 312

***webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Message to be sent is**
HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/
Content-Type: text/html
Content-Length: 312

<HTML><HEAD
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- send data length=448
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type External, but unable to get URL
*webauthRedirect: May 19 13:36:47.681: 0:17:7c:2f:b6:9a- received connection

*emWeb: May 19 13:36:48.731: SSL Connection created for MAC:0:17:7c:2f:b6:9a

*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- received connection

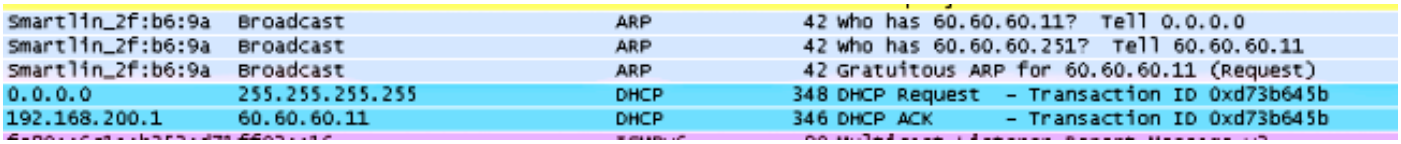
*webauthRedirect: May 19 13:36:51.795: captive-bypass detection disabled, Not checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- Preparing redirect URL according to configured Web-Auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Checking custom-web config for WLAN ID:4
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- unable to get the hostName for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Global status is enabled, checking on web-auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type Internal, no further redirection needed. Presenting defualt login page to user
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv= "Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body2 is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser host is www.facebook.com

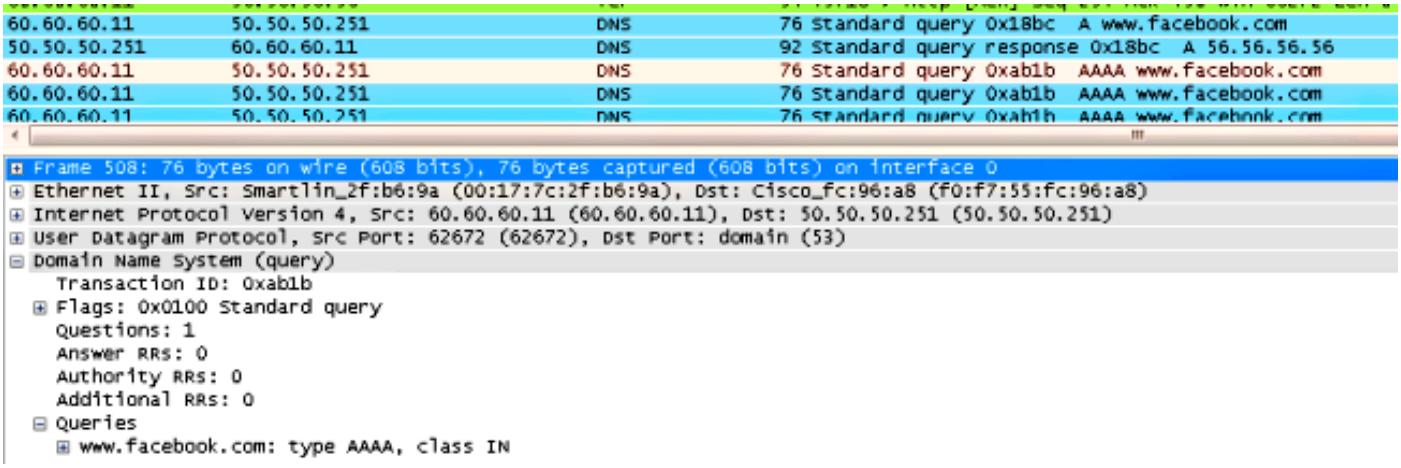
```
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser path is
/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- added redirect=, URL is
now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 323


*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Message to be sent is
 HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
Content-Type: text/html
Content-Length: 323


*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- send data length=470
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP received op
BOOTREQUEST (1) (len 308,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
           dhcpServer: 60.60.60.251, dhcpNetmask: 255.255.255.0,
           dhcpGateway: 60.60.60.251, dhcpRelay: 60.60.60.2  VLAN: 60


*emWeb: May 19 13:38:35.187:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1



*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:47.215:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created in mscb for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD
(8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a apfMsRunStateInc
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_NOL3SEC
(14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Session Timeout is 0 -
not starting session timer for the mobile
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Reached PLUMBFASTPATH: from line 6605
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Replacing Fast Path rule
  type = Airespace AP Client
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv6 ACL ID =
```

以下是客戶端資料包捕獲。

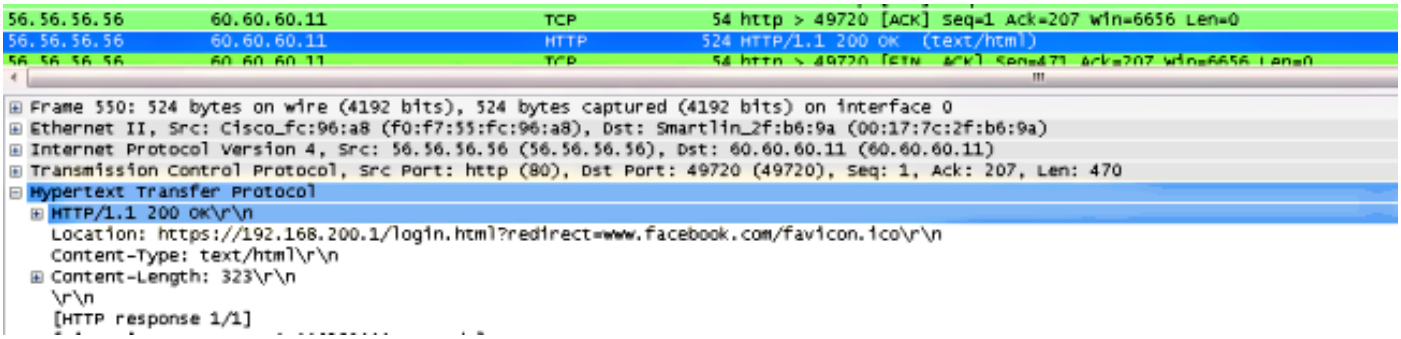
客戶端獲得IP地址。



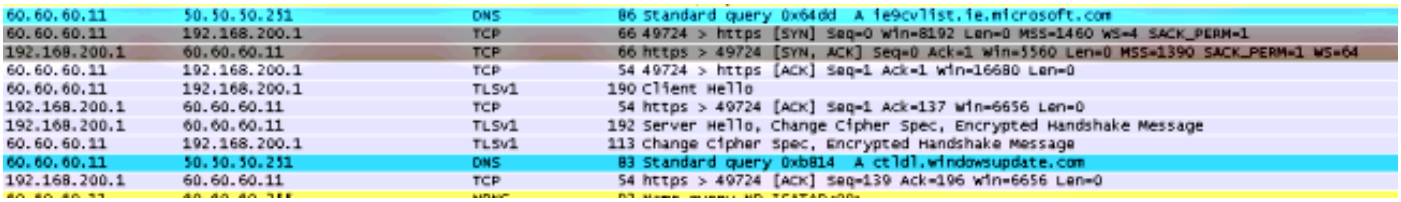
使用者端會開啟瀏覽器並輸入www.facebook.com。



WLC會攔截使用者端的首個TCP封包，並推送其虛擬IP位址和內部Webauth頁面。



成功進行Web身份驗證後，工作流的其餘部分完成。



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。